2876

PATENT
Attorney Docket No.: 4284.0829

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:			
TAKAFUMI WATANABE			
Serial No.:	09/498,995	Group Art Unit:	2876
Filed:	February 7, 2000	Examiner:	Unknown
For:	PORTABLE ELECTRONIC DEVICE AND A METHOD FOR ISSUING THE DEVICE		

CLAIM FOR PRIORITY

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Under the provisions of 35 U.S.C. § 119, Applicant hereby claims the benefit of the filing date of Japanese Application No. 11-029976, filed February 8, 1999, for the above-identified U.S. patent application.

In support of Applicant's claim for priority, filed herewith is one certified copy of the above.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Date: 4/12/00

By: _____
Richard V. Burgujian
Registration No. 31,744

LAW OFFICES
FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, D. C. 20005
202-408-4000

053
30030

日本国特許庁
PATENT OFFICE JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: １９９９年　２月　８日

出願番号
Application Number: 平成１１年特許願第０２９９７６号

出願人
Applicant (s): 株式会社東芝

２０００年　１月２１日

特許庁長官
Commissioner,
Patent Office 近藤隆彦

出証番号　出証特２０００－３０００３５０

【書類名】　特許願

【整理番号】　A009807072

【提出日】　平成11年 2月 8日

【あて先】　特許庁長官　殿

【国際特許分類】　G06K 19/00

【発明の名称】　携帯可能電子装置

【請求項の数】　9

【発明者】

【住所又は居所】　神奈川県川崎市幸区柳町７０番地　株式会社東芝柳町工場内

【氏名】　渡辺　隆文

【特許出願人】

【識別番号】　000003078

【氏名又は名称】　株式会社　東芝

【代理人】

【識別番号】　100058479

【弁理士】

【氏名又は名称】　鈴江　武彦

【電話番号】　03-3502-3181

【選任した代理人】

【識別番号】　100084618

【弁理士】

【氏名又は名称】　村松　貞男

【選任した代理人】

【識別番号】　100068814

【弁理士】

【氏名又は名称】　坪井　淳

【選任した代理人】

【識別番号】　100092196

【弁理士】

【氏名又は名称】　橋本　良郎

【選任した代理人】

【識別番号】　100091351

【弁理士】

【氏名又は名称】　河野　哲

【選任した代理人】

【識別番号】　100088683

【弁理士】

【氏名又は名称】　中村　誠

【選任した代理人】

【識別番号】　100070437

【弁理士】

【氏名又は名称】　河井　将次

【手数料の表示】

【予納台帳番号】　011567

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　携帯可能電子装置

【特許請求の範囲】

【請求項１】　不揮発性メモリとセキュリティ機能を有する携帯可能電子装置において、

上記不揮発性メモリにセキュリティ機能を有効化するか否かを示すデータを記憶する記憶手段と、

外部から供給される電文のフォーマットがセキュリティ用のデータを含むフォーマットか否かを判断する第１の判断手段と、

上記記憶手段により上記不揮発性メモリにセキュリティ機能の有効化を示すデータが記憶されているか否かを判断する第２の判断手段と、

上記第１の判断手段により電文のフォーマットがセキュリティ用のデータを含まないフォーマットと判断し、上記第２の判断手段によりセキュリティ機能の有効化を示すデータが記憶されていないと判断した際に、電文に基づいて不揮発性メモリに対する書き込みおよび書き換え処理を実行する第１の実行手段と、

上記第１の判断手段により電文のフォーマットがセキュリティ用のデータを含むフォーマットと判断した際に、電文に基づいてセキュリティ機能による検証に成功したか否かを判断する第３の判断手段と、

この第３の判断手段によりセキュリティ機能による検証に成功したと判断した際に、電文に基づいて不揮発性メモリに対する書き込みおよび書き換え処理を実行する第２の実行手段と、

を具備したことを特徴とする携帯可能電子装置。

【請求項２】　上記セキュリティ用のデータを含む電文のフォーマットが、書き込みおよび書き換えを示すコマンドと書き込みおよび書き換えの対象データとこの対象データの正当性を保証する補助データとからなり、上記セキュリティ機能は補助データの正当性の判断により行われることを特徴とする請求項１に記載の携帯可能電子装置。

【請求項３】　上記セキュリティ用のデータを含む電文のフォーマットが、書き込みおよび書き換えを示すコマンドと暗号化されている書き込みおよび書き

換えの対象データとからなり、上記セキュリティ機能は暗号化されている対象データの復号化により行われることを特徴とする請求項１に記載の携帯可能電子装置。

【請求項４】　上記セキュリティ用のデータを含む電文のフォーマットが、書き込みおよび書き換えを示すコマンドと暗号化されている書き込みおよび書き換えの対象データとこの暗号化されている対象データの正当性を保証する補助データとからなり、上記セキュリティ機能は補助データの正当性の判断と、暗号化されている対象データの復号化により行われることを特徴とする請求項１に記載の携帯可能電子装置。

【請求項５】　上記不揮発性メモリに複数のアプリケーションが記憶され、上記セキュリティ機能はアプリケーション毎に独立して設定可能であることを特徴とする請求項１に記載の携帯可能電子装置。

【請求項６】　上記記憶手段に記憶されているセキュリティ機能を有効化するか否かを示すデータはセキュリティ機能を有効化する電文を受信した場合に有効化することを特徴とする請求項１に記載の携帯可能電子装置。

【請求項７】　上記不揮発性メモリに複数のアプリケーションファイルが記憶されており、各アプリケーションファイル毎に処理される電文フォーマットを指定する指定情報が設定されていることを特徴とする請求項１に記載の携帯可能電子装置。

【請求項８】　上記第１の判断手段にてセキュリティ用のデータを含むフォーマットと判断し、かつ、上記第２の判断手段にて上記記憶手段にセキュリティ機能の有効化を示すデータが記憶されていないと判断した際に、用不揮発性メモリに複数のアプリケーションが記憶され、上記セキュリティ機能許容フォーマットでない旨の応答ステータスを出力することを特徴とする請求項１に記載の携帯可能電子装置。

【請求項９】　上記携帯可能電子装置は、ＩＣモジュールにより構成されていることを特徴とする請求項１に記載の携帯可能電子装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

この発明は、ＩＣカード等の携帯可能電子装置に関する。

【０００２】

【従来の技術】

ＩＣカード等の携帯可能電子装置では、暗証番号の照合や送信データの暗号化などにて実現されるセキュリティ機能にて、内部メモリに格納されているデータを不正な第三者が読み出し・書き込み・書き換えが出来ないような管理を行っている。

【０００３】

ＩＣカードは、所有者の暗証番号や暗号鍵などのアプリケーション運用に必要なデータを書き込むことにより使用可能な状態となる。この書き込み行為は一般に発行と呼ばれる。この発行時には不特定多数のカードに大量のデータを書くこととなるが、書き込みのためにはＩＣカードで要求されているセキュリテイ機能を満足する必要があり、データの暗号化など事前処理などを行うこととなるので非効率的である。

【０００４】

この結果、発行以前のカードでは要求されているセキュリティ機能を実現せずともデータの書き込みが行うことができ、すべてのデータが書き込まれた後にセキュリティ機能を有効化させることにより、それ以降のデータ書き込み・書き換えにはカードの要求するセキュリテイ機能の実現ができるものが要望されている。

【０００５】

すなわち、アプリケーション運用時には高セキュリティを実現でき、かつ、発行時の効率化を計ることが可能となるＩＣカードが要望されている。

【０００６】

【発明が解決しようとする課題】

この発明は、アプリケーション運用時には高セキュリティを実現でき、かつ、発行時の効率化を計ることが可能となるものが要望されているもので、アプリケーション運用時には高セキュリティを実現でき、かつ、発行時の効率化を計るこ

とが可能となる携帯可能電子装置を提供することを目的としている。

【０００７】

【課題を解決するための手段】

この発明の携帯可能電子装置は、不揮発性メモリとセキュリティ機能を有するものにおいて、上記不揮発性メモリにセキュリティ機能を有効化するか否かを示すデータを記憶する記憶手段と、外部から供給される電文のフォーマットがセキュリティ用のデータを含むフォーマットか否かを判断する第１の判断手段と、上記記憶手段により上記不揮発性メモリにセキュリティ機能の有効化を示すデータが記憶されているか否かを判断する第２の判断手段と、上記第１の判断手段により電文のフォーマットがセキュリティ用のデータを含まないフォーマットと判断し、上記第２の判断手段によりセキュリティ機能の有効化を示すデータが記憶されていないと判断した際に、電文に基づいて不揮発性メモリに対する書き込みおよび書き換え処理を実行する第１の実行手段と、上記第１の判断手段により電文のフォーマットがセキュリティ用のデータを含むフォーマットと判断した際に、電文に基づいてセキュリティ機能による検証に成功したか否かを判断する第３の判断手段と、この第３の判断手段によりセキュリティ機能による検証に成功したと判断した際に、電文に基づいて不揮発性メモリに対する書き込みおよび書き換え処理を実行する第２の実行手段とからなる。

【０００８】

【発明の実施の形態】

以下、この発明の実施形態について図面を参照して説明する。

【０００９】

図１は、この発明のＩＣカード（携帯可能電子装置）２を処理するＩＣカード処理装置１の全体構成を示すブロック図である。

【００１０】

このＩＣカード処理装置１には、装置全体の制御を司る端末３が設けられている。この端末３には、ＩＣカード２と端末３とを接続可能にし、ＩＣカード２とデータのやり取りを行うカードリーダ／ライタ４、コマンドやその他のデータを入力するキーボード５、各種データを表示するＣＲＴディスプレイ６、各種デー

タを印刷出力するプリンタ７、各種データを記憶するフロッピーディスク装置８がそれぞれ接続されている。上記カードリーダ／ライタ４は、コネクタ等の接触式あるいはアンテナを用いる無線式により、ＩＣカード２とデータのやり取りを行うようになっている。

【００１１】

図２は、ＩＣカード２の機能を概略的に示すブロック図である。すなわち、ＩＣカード２は、リーダ／ライタ部１１、暗証設定／暗証照合部１２、暗号化／復号化部１３等の基本機能を実行する部分と、これらの基本機能を管理するスーパーバイザ１０から構成されている。

【００１２】

上記リーダ／ライタ部１１は、上記端末３からカードリーダ／ライタ４を介して供給されたコマンド、データ等に基づき後述するデータメモリ１５あるいはプログラムメモリ１６からデータを読取ったり、書込んだりするものである。

【００１３】

上記暗証設定／暗証照合部１２は、暗証を設定したり暗証の照合を行うものである。

【００１４】

上記暗号化／復号化部１３は、上記端末３へ供給するデータを暗号化したり、上記端末３から供給された暗号化データを復号化するものである。

【００１５】

スーパーバイザ１０は、上記端末３からカードリーダ／ライタ４を介して供給された機能コードもしくはデータの付加された機能コードを解釈し、実行させるものである。

【００１６】

上記諸機能を発揮させるためにＩＣカード２は、図３に示すように、全体を制御する制御素子１４とデータメモリ１５とプログラムメモリ１６とコンタクト部１８からなる物理構成となっている。

【００１７】

データメモリ１５は、各種データの記憶に使用されＥＥＰＲＯＭ（不揮発性メ

モリ）で構成されている。プログラムメモリ１６はマスクＲＯＭで構成されたものであり、制御プログラムがあらかじめ記憶されているものである。コンタクト部１８は外部（カードリーダ／ライタ４）との接点となるものである。

【００１８】

上記制御素子１４、データメモリ１５、プログラムメモリ１６は１チップ状のＩＣ２０として形成されており、このＩＣ２０に外部とのインターフェイス部としてのコンタクト部１８が接続されて一体化（モジュール化）されたＩＣモジュール２１がプラスチックカードに埋め込まれることによりＩＣカード２が形成されている。

【００１９】

図４は、上記データメモリ１５の構成を示す図である。ＩＣカード２の運用時におけるデータメモリ１５のマッピング例である。

【００２０】

すなわち、データメモリ１５は、システムエリア１５ａ、ＤＦ（ディジネテッドファイル）、ＥＦ（エレメンタリーファイル）定義エリア１５ｂ、データエリア１５ｃの３つの領域からなる。

【００２１】

システムエリア１５ａは、ＩＣカード２が動作する上で必須な固定データおよび可変データの初期値から構成されている。システムエリア１５ａは、ＩＣカード２を運用するためには必須の領域であり、初期化時にデータが書き込まれている。

【００２２】

ＤＦ、ＥＦ定義エリア１５ｂは、ＤＦの定義情報と、このＤＦの子供に対応する少なくとも１つのＥＦ定義情報とが記録されるものである。図４の場合、ＤＦ１の定義情報に対して、ＥＦ１－１、ＥＦ１－２の２つのＥＦの定義情報が記録されている。この場合、ＤＦ１定義情報は、ＤＦ名”ＤＦ１”のＤＦ定義情報である。ＥＦ１－１定義情報およびＥＦ１－２定義情報は、それぞれＥＦ識別子”ＥＦ１”および”ＥＦ２”のＥＦ定義情報であり、双方ともにＤＦ１の配下に存在するものとする。ＤＦ、ＥＦ定義エリア１５ｂの未使用エリアは、新規に創成

されるＤＦおよびＥＦのための領域である。

【００２３】

また、データエリア１５ｃは、各ＥＦ定義情報で管理されるデータ本体が格納されている領域である。

【００２４】

データエリア１５ｃには、複数のアプリケーションが記憶され、各アプリケーションごとにＤＦ定義情報が付与されていることにより、アプリケーション毎に独立してセキュリティ機能の有効、無効を設定可能である。

【００２５】

図５を用いて上記ＤＦ定義情報の構成例を説明する。

【００２６】

上記ＤＦ定義情報は、ＤＦ名２１、ＤＦサイズ情報２２、セキュリティフォーマット情報２３、セキュリティフラグ２４により構成されている。

【００２７】

ＤＦ名２１はＤＦ毎にユニークな情報であり、この情報により処理対象のＤＦの検索を行う。ＤＦサイズ情報２２は当該ファイルが使用可能なデータメモリ１５の情報であり、当該ＤＦ配下にＥＦを創成した場合、その際に使用したサイズが当情報より減算される。セキュリティフォーマット情報２３は当該ＤＦ配下における書き込みおよび書き換え系コマンドの実現されるべき電文フォーマット（後述する）の情報が設定されている。

【００２８】

セキュリティフラグ２４は当ＤＦ定義情報が有効化されている際に立つものであり、このフラグにより当ＤＦ定義情報が有効化されている場合に、当該ＤＦ配下における書き込みおよび書き換え系コマンドではセキュリティフォーマット情報２３で指定される電文フォーマットは許可され、それ以外の電文フォーマットは拒絶されるものである。

【００２９】

図６を用いて上記ＤＦ配下に構築されるＥＦ定義情報の構成例を説明する。

【００３０】

ＥＦ定義情報は、ＤＦ識別情報３１、ＥＦ識別子３２、アドレス情報３３、ＥＦサイズ情報３４、ＥＦフォーマット情報３５により構成されている。

【００３１】

ＤＦ識別情報３１は当該ＥＦがどのＤＦの配下に存在するかを識別する情報である。ＥＦ識別子３２は各ＥＦ毎にユニークな情報であり、この情報により処理対象のＥＦを検索する。アドレス情報３３は当該ＥＦ制御情報で管理されるデータ格納領域の物理的アドレスを示す。ＥＦサイズ情報３４は当該ＥＦ制御情報で管理されるデータ格納領域のサイズ情報を示す。ＥＦフォーマット情報３５は当該ＥＦ制御情報が、例えば、ＩＳＯ７８１６－４で規定されているレコード構造ＥＦかあるいはトランスペアレント構造ＥＦなのかの情報を与えるものである。

図７の（ａ）～（ｄ）を用いて書き込みおよび書き換え系コマンドの実現されるべき電文フォーマットを説明する。

【００３２】

図７の（ａ）に示すフォーマット＃１は、書き込みおよび書き換え系コマンドの基本的なフォーマットであり、書き込みおよび書き換えを示すコマンドとしてのコマンドヘッダ部と書き込みおよび書き換えの対象データとしてのデータ部とからなり、上記のセキュリティフラグ２４が有効化されていない場合にのみ許容されるものである。

【００３３】

図７の（ｂ）に示すフォーマット＃２は、データの隠蔽性を実現するために暗号化データ部を有するフォーマットであり、書き込みおよび書き換えを示すコマンドとしてのコマンドヘッダ部と暗号化されている書き込みおよび書き換えの対象データとしての暗号化データ部とからなる。このフォーマットの場合、暗号化されている書き込みおよび書き換えの対象データの復号化によりセキュリティ機能の検証が行われる。

【００３４】

図７の（ｃ）に示すフォーマット＃３は、データの正当性を実現するために補助データ部を有するフォーマットであり、書き込みおよび書き換えを示すコマンドとしてのコマンドヘッダ部と書き込みおよび書き換えの対象データとしてのデ

ータ部と対象データの正当性を保証する補助データ部とからなる。このフォーマットの場合、補助データの正当性の判断によりセキュリティ機能の検証が行われる。

【００３５】

図７の（ｄ）に示すフォーマット＃４は、データの隠蔽性および完全性を実現するために暗号化データ部を有し、かつ、補助データ部を有するフォーマットであり、書き込みおよび書き換えを示すコマンドとしてのコマンドヘッダ部と暗号化されている書き込みおよび書き換えの対象データとしての暗号化データ部と暗号化されている対象データの正当性を保証する補助データ部とからなる。このフォーマットの場合、暗号化されている書き込みおよび書き換えの対象データの復号化と、補助データの正当性の判断とによりセキュリティ機能の検証が行われる。

【００３６】

上記フォーマット＃１～＃３は、上記セキュリティフォーマット情報２３にて各ＤＦ毎に指定されるようになっている。

【００３７】

図８に上記セキュリティフラグ２４を有効化するコマンドの電文フォーマットを示す。このコマンドは、コマンドヘッダ部のみにより構成されている。

【００３８】

当該コマンドが実行された直後より、ＤＦ定義情報のセキュリティフラグ２４が有効化されるようになっている。

【００３９】

次に、ＤＦ定義情報のセキュリティフラグ２４を有効化する処理を、図９に示すフローチャートを参照しつつ説明する。

【００４０】

すなわち、端末３からセキュリティフラグを有効化するコマンドの電文（図８参照）が、カードリーダ／ライタ４をコンタクト部１８を介してＩＣカード２内の制御素子１４に送信される。これにより、制御素子１４は端末３から送信された電文を受信し（ＳＴ１）、この受信した電文が、セキュリティフラグを有効化

するコマンドと判断した際に（ＳＴ２）、現在処理中（カレント状態）のＤＦ定義情報内のセキュリティフラグ２４を有効化する（ＳＴ３）。

【００４１】

次に、書き込みおよび書き換え系コマンドによる処理を、図１０に示すフローチャートを参照しつつ説明する。

【００４２】

すなわち、端末３から書き換えおよび書込み系コマンドの電文（図７の（ａ）～（ｄ）参照）が、カードリーダライタ４をコンタクト部３５を介してＩＣカード２内の制御素子１４に送信される。これにより、制御素子１４は端末３から送信された電文を受信し（ＳＴ１１）、この受信した電文フォーマット内容を判断する（ＳＴ１２）。これにより、制御素子１４は、図７の（ａ）に示すフォーマット＃１と判断した際に、現在処理中（カレント状態）のＤＦ定義情報内のセキュリティフラグ２４を有効化済みか否かを判断する（ＳＴ１３）。この判断により、セキュリティフラグ２４を有効化済みでないと判断された際に、制御素子１４は、コマンドヘッダ部により指定されている書き換えおよび書込み処理を実行する（ＳＴ１４）。

【００４３】

これにより、発行以前のＩＣカード２において、要求されているセキュリティ機能を実現せずに、データの書き換えおよび書き込みが行うことができ、発行時の効率化を計ることが可能となる。

【００４４】

また、上記ステップ１３によりセキュリティフラグ２４を有効化済みと判断された際に、制御素子１４は、「許容フォーマットでない」の応答ステータスを端末３へ送信する（ＳＴ１５）。これにより、フォーマット＃１は、当該ＤＦ制御情報のセキュリティフラグ２４が有効化されている場合に拒絶される。

【００４５】

また、上記ステップ１２により電文がフォーマット＃１と判断しなかった際に、制御素子１４は、現在処理中（カレント状態）のＤＦ定義情報内のセキュリティフォーマット情報２３に基づいて指定される処理を、受信した電文を用いて実

施する（ＳＴ１６）。

【００４６】

この処理により、制御素子１４は、セキュリティ機能による検証に成功したか否かを判断する（ＳＴ１７）。この判断の結果、セキュリティ機能による検証に成功した際、制御素子１４は、コマンドヘッダ部により指定されている書き換えおよび書込み処理を実行する（ＳＴ１４）。

【００４７】

これにより、ＩＣカード２の発行後のデータ書き込み・書き換えに対して、カードの要求するセキュリテイ機能を実現できる。

【００４８】

また、上記ステップ１７によりセキュリティ機能による検証に成功しなかった際に、制御素子１４は、「受信した電文の正当性の検証に失敗」の応答ステータスを端末３へ送信する（ＳＴ１８）。

【００４９】

上記したように、発行以前のＩＣカードでは要求されているセキュリティ機能を実現せずともデータの書き込みが行うことができ、すべてのデータが書き込まれた後にセキュリティ機能を有効化させることにより、それ以降のデータ書き込み・書き換えにはＩＣカードの要求するセキュリテイ機能の実現が必須となる。すなわち、アプリケーション運用時には高セキュリティを実現でき、かつ、発行時の効率化を計ることが可能となる。

【００５０】

【発明の効果】

以上詳述したように、この発明によれば、アプリケーション運用時には高セキュリティを実現でき、かつ、発行時の効率化を計ることが可能となる携帯可能電子装置を提供できる。

【図面の簡単な説明】

【図１】

この発明のＩＣカード処理装置の全体構成を示すブロック図。

【図２】

ＩＣカードの機能を概略的に示すブロック図。

【図３】

ＩＣカードの構成を概略的に示すブロック図。

【図４】

データメモリの構成を示す図。

【図５】

ＤＦ定義情報の構成例を示す図。

【図６】

ＥＦ定義情報の構成例を示す図。

【図７】

書き込みおよび書き換え系コマンドの実現されるべき電文フォーマットを示す図。

【図８】

セキュリティフラグを有効化するコマンドの電文フォーマットを示す図。

【図９】

ＤＦ定義情報のセキュリティフラグを有効化する処理を説明するためのフローチャート。

【図１０】

書き込みおよび書き換え系コマンドによる処理を説明するためのフローチャート。

【符号の説明】

１…ＩＣカード処理装置

２…ＩＣカード（携帯可能電子装置）

３…端末

４…カードリーダ／ライタ

１１…リーダ／ライタ

１４…制御素子

１５…データメモリ

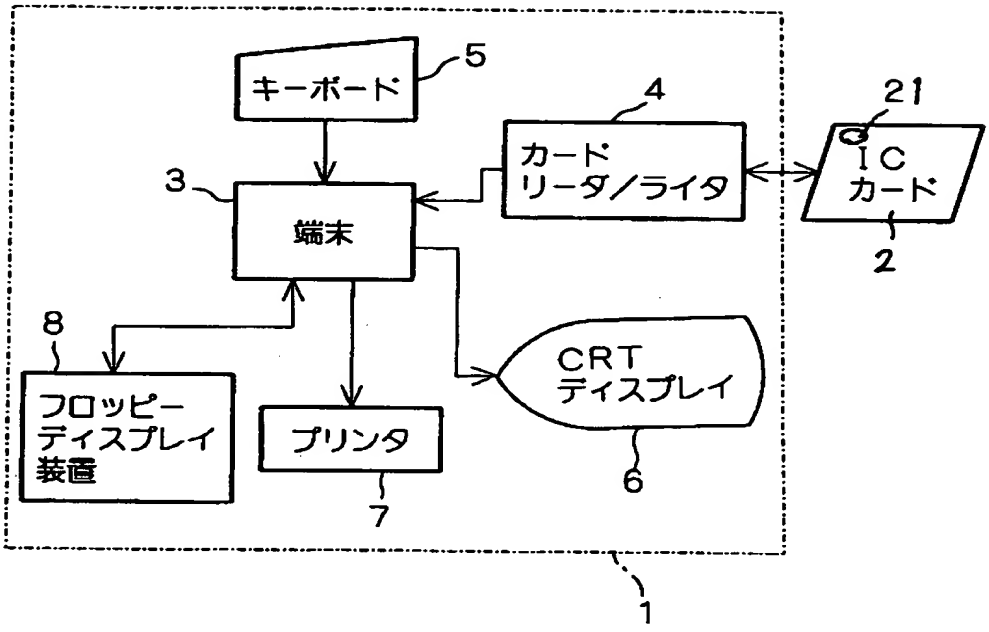
１５ａ…システムエリア

１５ｂ…ＤＦ、ＥＦ定義エリア

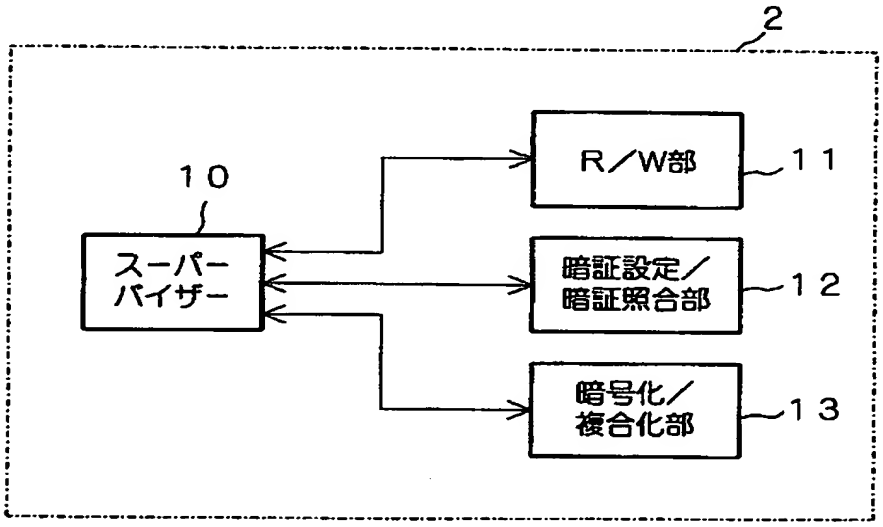
１５ｃ…データエリア

【書類名】　　図面

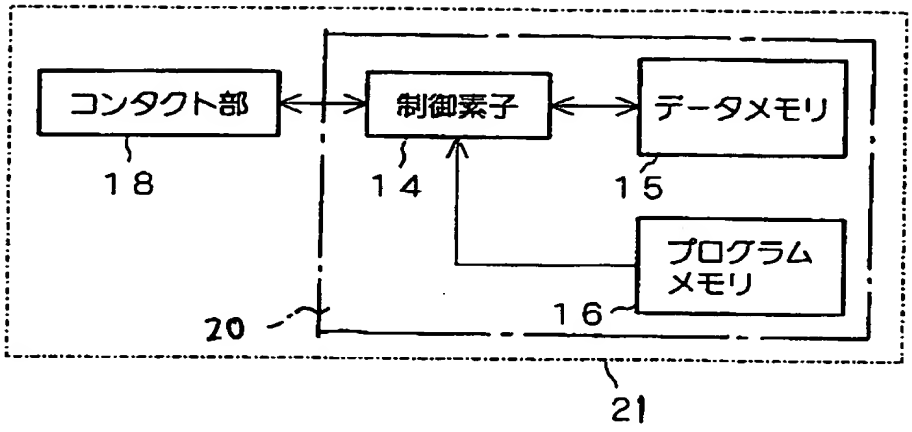
【図１】


キーボード
5
4
21
カード
リーダ／ライタ
IC
カード
3
端末
2
8
CRT
ディスプレイ
フロッピー
ディスプレイ
装置
プリンタ
6
7
1

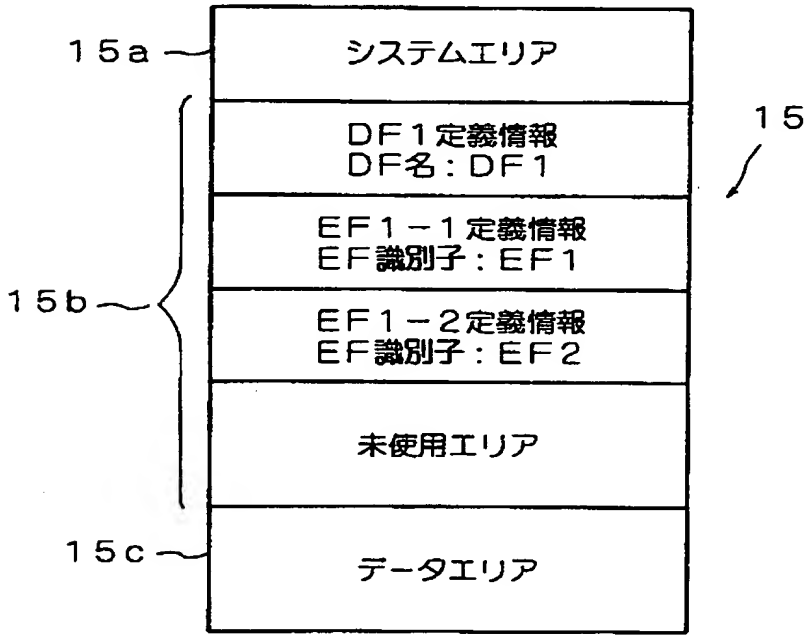
【図２】


2
R／W部
11
10
スーパー
バイザー
暗証設定／
暗証照合部
12
暗号化／
複合化部
13

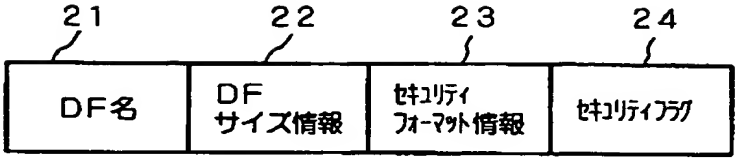
【図３】


コンタクト部
制御素子
データメモリ
18
14
15
プログラム
メモリ
16
20
21

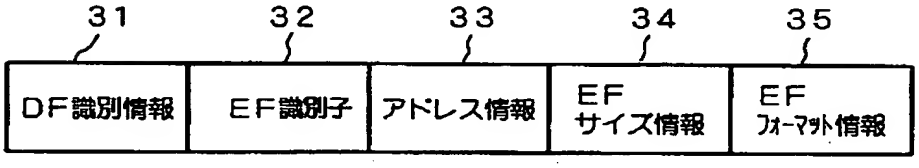
【図４】


15a
システムエリア
DF1定義情報
DF名：DF1
15
EF1－1定義情報
EF識別子：EF1
15b
EF1－2定義情報
EF識別子：EF2
未使用エリア
15c
データエリア

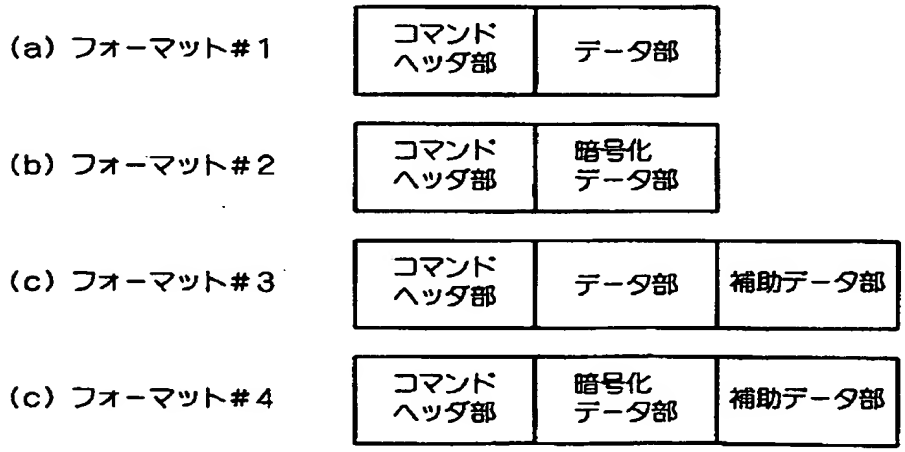
【図５】


21
22
23
24
DF名
DF
サイズ情報
セキュリティ
フォーマット情報
セキュリティフラグ

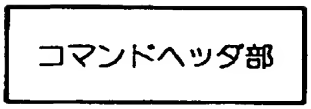
【図６】


31
32
33
34
35
DF識別情報
EF識別子
アドレス情報
EF
サイズ情報
EF
フォーマット情報

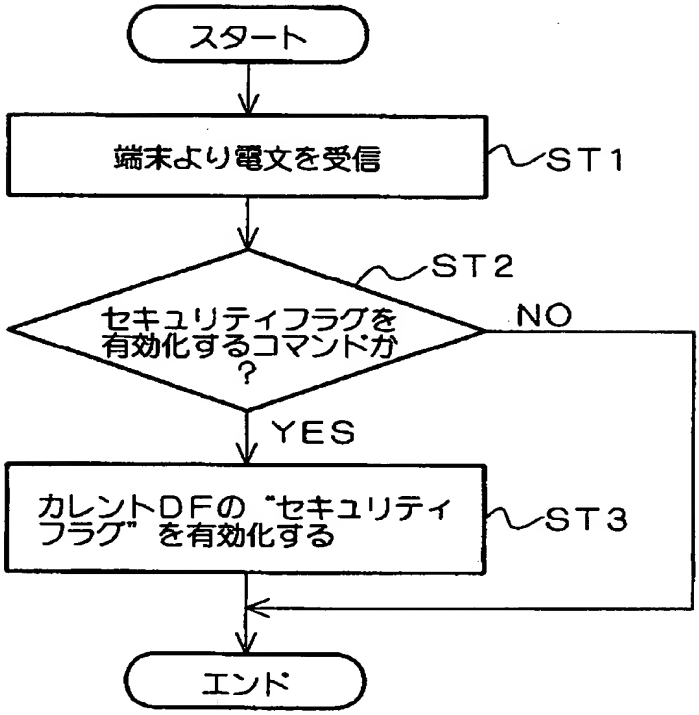
【図７】


(a) フォーマット#1
コマンド
ヘッダ部
データ部
(b) フォーマット#2
コマンド
ヘッダ部
暗号化
データ部
(c) フォーマット#3
コマンド
ヘッダ部
データ部
補助データ部
(c) フォーマット#4
コマンド
ヘッダ部
暗号化
データ部
補助データ部

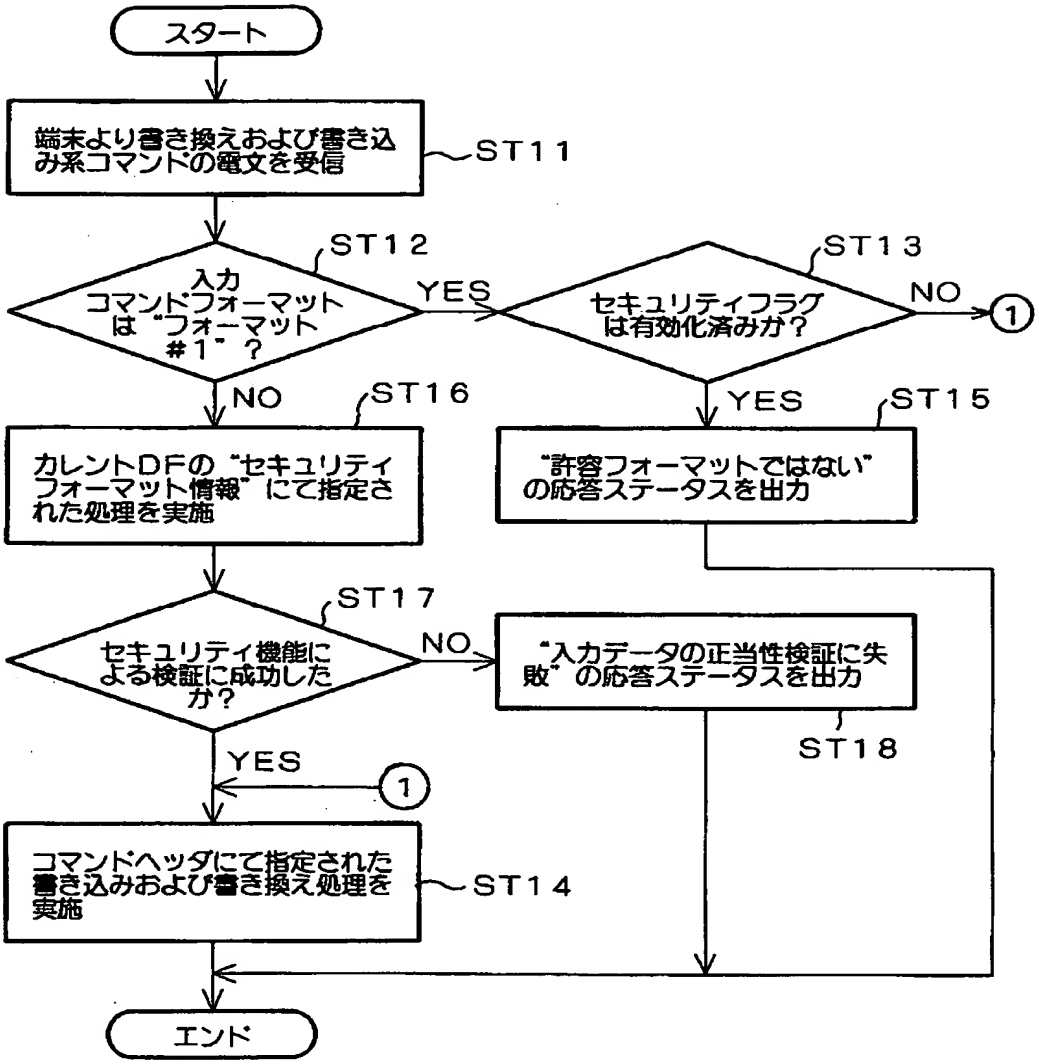
【図８】


コマンドヘッダ部

【図９】


スタート
端末より電文を受信
ST1
ST2
セキュリティフラグを有効化するコマンドか？
NO
YES
カレントDFの"セキュリティフラグ"を有効化する
ST3
エンド

【図１０】


スタート
端末より書き換えおよび書き込み系コマンドの電文を受信
ST11
入力コマンドフォーマットは“フォーマット#1”？
ST12
YES
セキュリティフラグは有効化済みか？
ST13
NO
①
NO
ST16
YES
ST15
カレントDFの“セキュリティフォーマット情報”にて指定された処理を実施
“許容フォーマットではない”の応答ステータスを出力
ST17
セキュリティ機能による検証に成功したか？
NO
“入力データの正当性検証に失敗”の応答ステータスを出力
ST18
YES
①
コマンドヘッダにて指定された書き込みおよび書き換え処理を実施
ST14
エンド

【書類名】　　要約書

【要約】

【課題】　この発明は、アプリケーション運用時には高セキュリティを実現でき、かつ、発行時の効率化を計ることが可能となる。

【解決手段】　この発明は、発行以前のＩＣカードでは要求されているセキュリティ機能を実現せずともデータの書き込みが行うことができ、すべてのデータが書き込まれた後にセキュリティ機能を有効化させるようにしたものである。

【選択図】　　図３

出　願　人　履　歴　情　報

識別番号　　〔０００００３０７８〕

１．変更年月日　　１９９０年　８月２２日
［変更理由］　新規登録
住　所　神奈川県川崎市幸区堀川町７２番地
氏　名　株式会社東芝